BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 790 347**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **99 02364**

(51) Int Cl[7] : **H 04 L 12/22**, H 04 L 9/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 25.02.99.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 01.09.00 Bulletin 00/35.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *STMICROELECTRONICS SA Société anonyme* — FR.

(72) **Inventeur(s)** : ROMAIN FABRICE.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : CABINET BALLOT SCHMIT.

(54) PROCEDE DE SECURISATION D'UN ENCHAINEMENT D'OPERATIONS REALISEES PAR UN CIRCUIT ELECTRONIQUE DANS LE CADRE DE L'EXECUTION D'UN ALGORITHME.

(57) L'invention concerne un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme. Le procédé selon l'invention fait intervenir une étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices dans l'enchaînement d'opérations, afin d'empêcher un accès frauduleux, par une analyse statistique de courants électriques, à des données protégées.

FR 2 790 347 - A1

PROCEDE DE SECURISATION D'UN ENCHAINEMENT D'OPERATIONS REALISEES PAR UN CIRCUIT ELECTRONIQUE DANS LE CADRE DE L'EXECUTION D'UN ALGORITHME

La présente invention se rapporte à un procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Plus particulièrement, l'invention concerne un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, la sécurisation étant apportée par la présence d'informations parasites qui gênent l'observation, depuis l'extérieur du circuit électronique, des manifestations physiques associées à l'exécution des opérations utiles.

Dans le cadre de l'invention, un algorithme doit être compris en tant qu'enchaînement d'actions nécessaires à l'accomplissement d'une tâche. Il ne s'agit par conséquent pas nécessairement de la mise en oeuvre d'un programme informatique.

Le domaine d'application de l'invention est essentiellement le domaine de la cryptologie. La cryptologie peut se définir comme étant la science de la dissimulation de l'information. Elle constitue, avec la sécurité physique des composants et des systèmes d'exploitation, la dimension essentielle de la sécurité des cartes à puces. La cryptologie englobe la cryptographie, qui est l'art de chiffrer et de déchiffrer des messages, et la cryptanalyse, qui est l'art de casser les codes secrets.

Dans les cartes à puce, la cryptographie met en oeuvre divers mécanismes qui ont pour but d'assurer soit la confidentialité des informations, soit

l'authentification des cartes ou des utilisateurs, soit encore la signature des messages.

L'ensemble des moyens mettant en oeuvre la cryptographie forme un crypto-système. De tels crypto-systèmes renferment des informations confidentielles, notamment pour chiffrer et déchiffrer des messages numériques.

Parmi ces informations confidentielles, on peut citer les clés de chiffrement et de déchiffrement, qui sont des paramètres d'une convention secrète utilisée pour le chiffrement et le déchiffrement de messages numériques.

L'utilisation de ces clés de chiffrement et de déchiffrement nécessite souvent plusieurs transferts des données les caractérisant. Lors de leur utilisation au sein d'un crypto-système, les données caractéristiques de clés numériques et d'autres informations confidentielles circulent entre différents registres et modules de mémoire ou de traitement. Ces transferts entre registres et/ou modules se traduisent par l'apparition de courants électriques ou de champs magnétiques porteurs d'informations confidentielles. Les informations confidentielles peuvent, par exemple, concerner des clés de chiffrement et de déchiffrement.

De tels crypto-systèmes posent un problème de visibilité depuis le monde extérieur. En effet, une mesure des signaux électriques ou des champs magnétiques nés des échanges d'informations entre différentes parties du circuit peut permettre d'accéder à des informations confidentielles qui participent à la protection de données par le système de chiffrement ou de déchiffrement.

En effet, au moment de l'utilisation de la clé numérique par un composant habilité tel qu'une carte à puce, une certaine visibilité, par exemple sur la clé

numérique, est rendue possible par l'étude de tels signaux électriques. Les signaux électriques sensibles peuvent être observés sur différents bus de communication reliant différents registres ou modules de mémoire ou de traitement.

Une clé numérique peut ainsi être découverte suite à une accumulation de mesures de signaux électriques ou magnétiques et à une étude statistique de ces mesures.

D'une façon plus générale, tout circuit électronique a une consommation électrique liée aux opérations qu'il effectue. Il est possible, en mesurant cette consommation, de découvrir des informations cachées dans le circuit. Ce problème se pose en tout composant sécurisé, et notamment les composants pour cartes à puce.

La découverte de données protégées par observation de courant nécessite en général une reproductibilité de la mesure de courant afin d'effectuer les traitements statistiques.

Ainsi, lorsqu'un circuit électronique exécute un algorithme contenant des opérations identiques ou voisines, et répétitives, telles que des transferts de données confidentielles entre registres, et où l'observation fine des opérations une par une peut révéler une information confidentielle, une analyse statistique fondée sur la mesure des courants électriques précédemment cités peut nuire à la sécurité du circuit électronique.

La présente invention a pour objet de pallier les problèmes qui viennent d'être décrits.

L'invention propose donc une méthode permettant de parer à une divulgation, par observation du courant, de données protégées.

A cet effet, l'invention propose un procédé de sécurisation d'un enchaînement d'opérations réalisées

par un circuit électronique dans le cadre de l'exécution d'un algorithme qui assure la non-visibilité vis-à-vis d'une analyse des signaux électriques lors des transferts de données entre différents registres.

Pour atteindre ces objectifs, l'invention propose d'insérer des opérations factices dans un enchaînement d'opérations utiles, de même type, effectuées dans le cadre de l'exécution d'un algorithme. Les opérations factices sont très ressemblantes aux opérations utiles. Chaque opération factice est insérée à un rang aléatoire pour chaque exécution de l'algorithme. Ainsi, l'acquisition de mesures de courant comparables devient très difficile.

L'invention concerne donc un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations utiles.

Les différents aspects et avantages de l'invention apparaîtront plus clairement dans la suite de la description, qui présente un exemple de mise en oeuvre préféré du procédé selon l'invention et qui n'est donné qu'à titre indicatif et nullement limitatif de l'invention.

Selon un mode préféré de l'invention, un certain nombre d'opérations factices sont insérées entre des opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme. Ces opérations factices sont introduites de façon aléatoire : ces opérations factices peuvent être

introduites entre n'importe quelle opération utile associée à l'algorithme.

On peut également trouver une ou plusieurs opérations factices avant la première opération utile associée à un algorithme ou après la dernière opération utile associée à un algorithme. On peut également trouver plusieurs opérations factices consécutives.

Afin de donner des séries de mesure de courant différentes à chaque exécution d'un même algorithme, de nouveaux aléas sont introduits à chaque exécution d'un algorithme.

Néanmoins, dans une application préférée, le procédé selon l'invention comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations, qu'elles soient utiles et/ou factices successives. Ainsi, l'insertion des opérations factices n'apparaît pas de façon évidente lors d'une étude temporelle des signaux électriques associés aux opérations utiles réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Enfin, il est préférable, mais pas obligatoire, que le nombre d'opérations factices introduites dans l'enchaînement d'opérations utiles soit constant pour chaque nouvelle exécution de l'algorithme. Ainsi, le temps d'exécution de l'algorithme dans sa totalité est le même à chaque exécution de l'algorithme. Le fait que des opérations factices ont été introduites est ainsi invisible en première analyse, ce qui assure encore une meilleure sécurisation de l'enchaînement d'opérations utiles.

Selon l'invention, il est également possible de distribuer les aléas seulement sur certaines parties de l'algorithme. De plus, le procédé selon l'invention peut également s'appliquer à des algorithmes dont les

opérations sont ordonnées, c'est-à-dire que les opérations utiles doivent s'enchaîner dans un ordre qu'on ne peut pas changer.

Le nombre d'opérations factices introduites est, dans une application préférée de l'invention, de l'ordre de 2 pourcent sur le nombre total d'opérations effectuées.

REVENDICATIONS

1. Procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations.

2. Procédé de sécurisation d'un enchaînement d'opérations de même type selon la revendication 1, caractérisé en ce que le procédé comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations utiles et/ou factices successives.

3. Procédé de sécurisation d'un enchaînement d'opérations de même type selon l'une des revendications 1 ou 2, caractérisé en ce que le nombre d'opérations factices introduites dans l'enchaînement d'opérations est constant pour chaque nouvelle exécution de l'algorithme.

4. Utilisation du procédé selon l'une des revendications précédentes dans le domaine de la cryptographie.

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2790347

N° d'enregistrement national

FA 573582
FR 9902364

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 septembre 1997 (1997-09-12) * abrégé * * page 1, ligne 1 - page 2, ligne 21 * * page 3, ligne 11 - ligne 29 *	1,4
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 septembre 1991 (1991-09-25) * colonne 1, ligne 1 - colonne 3, ligne 1 * * colonne 6, ligne 38 - ligne 52 *	1
A		2
A	COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAM EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 12, no. 6, page 565-584 XP000415701 ISSN: 0167-4048 * page 568, colonne de gauche, alinéa 3 - page 569, colonne de droite, alinéa 2 * * page 570, colonne de droite, alinéa 3 * * page 571, colonne de droite, alinéa 3 - page 572, colonne de gauche, alinéa 2 *	2,3
A	DALLAS SEMICONDUCTOR CORP.: "SECTION 1: INTRODUCTION" 6 octobre 1993 (1993-10-06) , DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3,7,8,73,77-80,82,152-156,229,290-292 XP002053731 * page 78 *	2

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04L
G06F

1

Date d'achèvement de la recherche	Examinateur
12 novembre 1999	Powell, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)